REMARKS

Claims 1, 4-7, 10, 12-14, 16, 18, 22-25, 27, 29, 31-33, 36, 38-39, 41, 43-44, 47, 50-51, 53-54, and 56-65 have been amended. Claims 1-65 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Section 101 Rejection:

The Examiner rejected claims 1-65 under 35 U.S.C. § 101 as being based on non-statutory subject matter. Specifically, the Examiner submits that the claimed invention is directed toward nothing more than the abstract idea of a mathematical algorithm. Applicants respectfully traverse this rejection. However, to expedite prosecution, independent claims 1 and 18 have been amended. Specifically, claims 1 and 18 have been amended to recite a method implemented in a device supporting a cryptography application, and to recite limitations involving the use of a generated result in a cryptography application.

Applicants respectfully remind that Examiner that in *State Street Bank & Trust Co. v. Signature Financial Group, Inc.*, 149 F.3d 1368, 47 USPQ2d 1596 (Fed. Cir. 1998), as discussed in MPEP 2106, the court stated that the relevant claim was statutory because "the transformation of data, representing discrete dollar amounts, by a machine through a series of mathematical calculations into a final share price, constitutes a practical application … because it produces 'a useful, concrete and tangible result' – a final share price". Just like transforming data representing discrete dollar amounts to determine a final share price was considered a practical application and thus statutory in *State Street*, the generation, storage, and use of computation results in a cryptography application is a practical application and thus statutory. Claims 1 and 18 clearly recite a practical application in the technological arts.

Applicants note that claims 43-56, 64, and 65 recite a processor comprising an arithmetic circuit for implementing methods similar to those recited in claims 1-42, and

are therefore directed toward statutory subject matter. Independent claims 57 and 61 have been amended to more clearly indicate that claims 57-63 are directed to a storage medium comprising program instructions executable by a processor supporting a cryptography application that cause the processor to implement methods similar to those recited in claims 1-42. For reasons similar to those discussed above, Applicants assert that these claims are also directed to statutory subject matter.

For at least the reasons above, Applicants respectfully request the removal of the rejection of claims 1-65 under 35 U.S.C. § 101.

Section 102(e) Rejection:

The Examiner rejected claims 1-65 under 35 U.S.C. § 102(e) as being anticipated by Gressel et al. (U.S. Patent 6,748,410) (hereinafter "Gressel"). Applicants respectfully traverse this rejection for at least the following reasons.

Regarding claims 1-17, contrary to the Examiner's assertion, Gressel fails to disclose all the limitations of these claims. The Examiner cites various passages in Gressel as teaching: acceleration, improvements of arithmetic operations, arithmetic operations utilized to generate cryptographic key(s), processor utilization for key generation, XOR operation, multiplication of two values, and sum of two values utilizing partial (i.e., any bit length) result from previous multiplication. The Examiner submits, therefore, that Gressel teaches the limitations of claim 1, in its original form. Applicants note that the Examiner has failed to address each and every limitation of independent claim 1, and each limitation of dependent claims 2-17 in his remarks. For example, the Examiner's remarks as to the teachings of these passages do not address all of the specific limitations of claim 1, such as "adding implicitly a partial result from a previously executed single arithmetic instruction to generate a result that represents the first number multiplied by the second number summed with the partial result." Instead, the Examiner submits that Gressel teaches, "multiplication two values, sum two values utilizing partial (i.e. any bit length) result from previous multiplication," which is clearly

not what is recited in claim 1. Similarly, many of the limitations of claims 2-17 are not mentioned at all in the Examiner's remarks. Applicants note MPEP 707.07(d), which requires that, in an Examiner's Action, the ground of rejection, should be "fully and clearly stated". **Since the rejection of claims 1-17 has not been fully and clearly stated, Applicants assert that it is improper.**

Further regarding claim 1, Applicants assert that the cited passages do not teach all of the specific limitations of this claim. For example, the Examiner equates adding a value of "any bit length" to the limitation, "adding implicitly a partial result from a previously executed single arithmetic instruction to generate a result that represents the first number multiplied by the second number summed with the partial result, wherein said partial result comprises a high order portion of a result of the previously executed single arithmetic instruction." **A value of "any bit length" clearly does not teach the specific limitations of the partial result recited claim 1, i.e., *wherein said partial result comprises a high order portion of a result of the previously executed single arithmetic instruction*.** In addition, Applicants assert that the cited passages do not teach the additional limitations, **"*storing at least a portion of the generated result; and using the stored at least a portion of the generated result in a subsequent computation in a cryptography application*,"** as recited in claim 1.

Applicants remind the Examiner that anticipation requires the presence in a single prior art reference disclosure of each and every limitation of the claimed invention, arranged as in the claim. M.P.E.P 2131; *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984). The **identical invention** must be shown in as complete detail as is contained in the claims. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). As discussed above, Gressel clearly does not disclose all of the specific limitations of claim 1.

Applicants assert that numerous ones of dependent claims 2-17 recite further distinctions over the cited art. Applicants traverse the rejection of these claims for at least the reasons given above in regard to claim 1, from which they depend. However,

since the rejections have been shown to be unsupported for independent claim 1, a further discussion of these dependent claims is not necessary at this time. Applicants reserve the right to present additional arguments.

For at least the reasons above, the rejection of claims 1-17 is unsupported by the cited art and removal thereof is respectfully requested.

Independent claims 43, 57, and 64 include limitations similar to those of claim 1, and so the arguments presented above apply with equal force to these claims as well.

Regarding claims 18-42, the Examiner cites the same passages and includes the same remarks about their teachings as in his rejection of claims 1-17. Applicants traverse this rejection for at least the reasons presented above regarding limitations in these claims that are similar to those in claims 1-17. In addition, Applicants assert that claims 18-42 recite different limitations than claims 1-17 that are not addressed by the Examiner, nor taught by Gressel. For example, claim 18 includes the limitation, "adding a third number to generate a result that represents the first number multiplied by the second number summed with the partial result and the third number." This limitation is not discussed in the Examiner's remarks, which include only a generic reference to Gressel teaching, "multiplication two values, sum to values utilizing partial (i.e. any bit length) result from previous multiplication." **The cited passages teach nothing about the above-referenced limitation of claim 18.**

Applicants again assert that the Examiner has failed to fully and clearly state his ground of rejection for claims 18-42. Applicants further assert that numerous ones of dependent claims 19-42 recite further distinctions over the cited art. Applicants traverse the rejection of these claims for at least the reasons given above in regard to claim 18, from which they depend. However, since the rejections have been shown to be unsupported for independent claim 18, a further discussion of these dependent claims is not necessary at this time. Applicants reserve the right to present additional arguments.

For at least the reasons above, the rejection of claims 18-42 is unsupported by the cited art and removal thereof is respectfully requested.

Independent claims 50, 61, and 65 include limitations similar to those of claim 18, and so the arguments presented above apply with equal force to these claims as well.

Applicants further assert that numerous other ones of the dependent claims recite further distinctions over the cited art. Applicants traverse the rejection of these claims for at least the reasons given above in regard to the claims from which they depend. However, since the rejections have been shown to be unsupported for the independent claims, a further discussion of the dependent claims is not necessary at this time. Applicants reserve the right to present additional arguments.

CONCLUSION

Applicants respectfully submit that the application is in condition for allowance, and prompt notice to that effect is respectfully requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/6000-32301/RCK.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Applicants

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: July 2, 2007